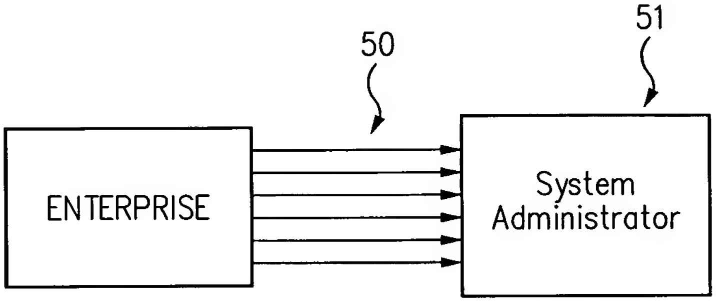


FIG. 1
(PRIOR ART)

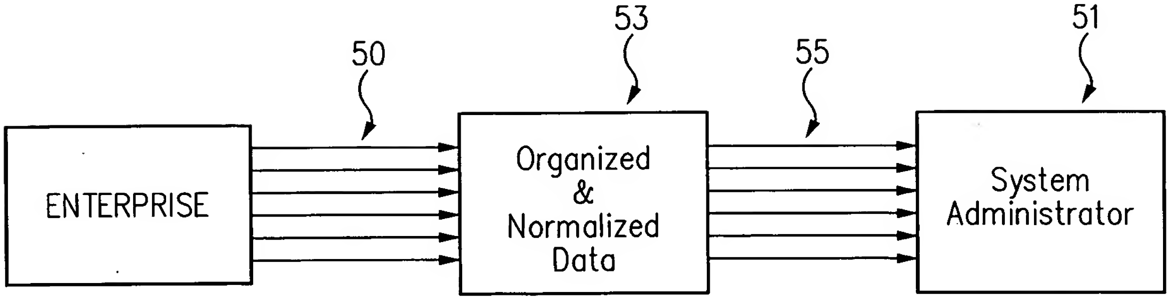


FIG. 2
(PRIOR ART)

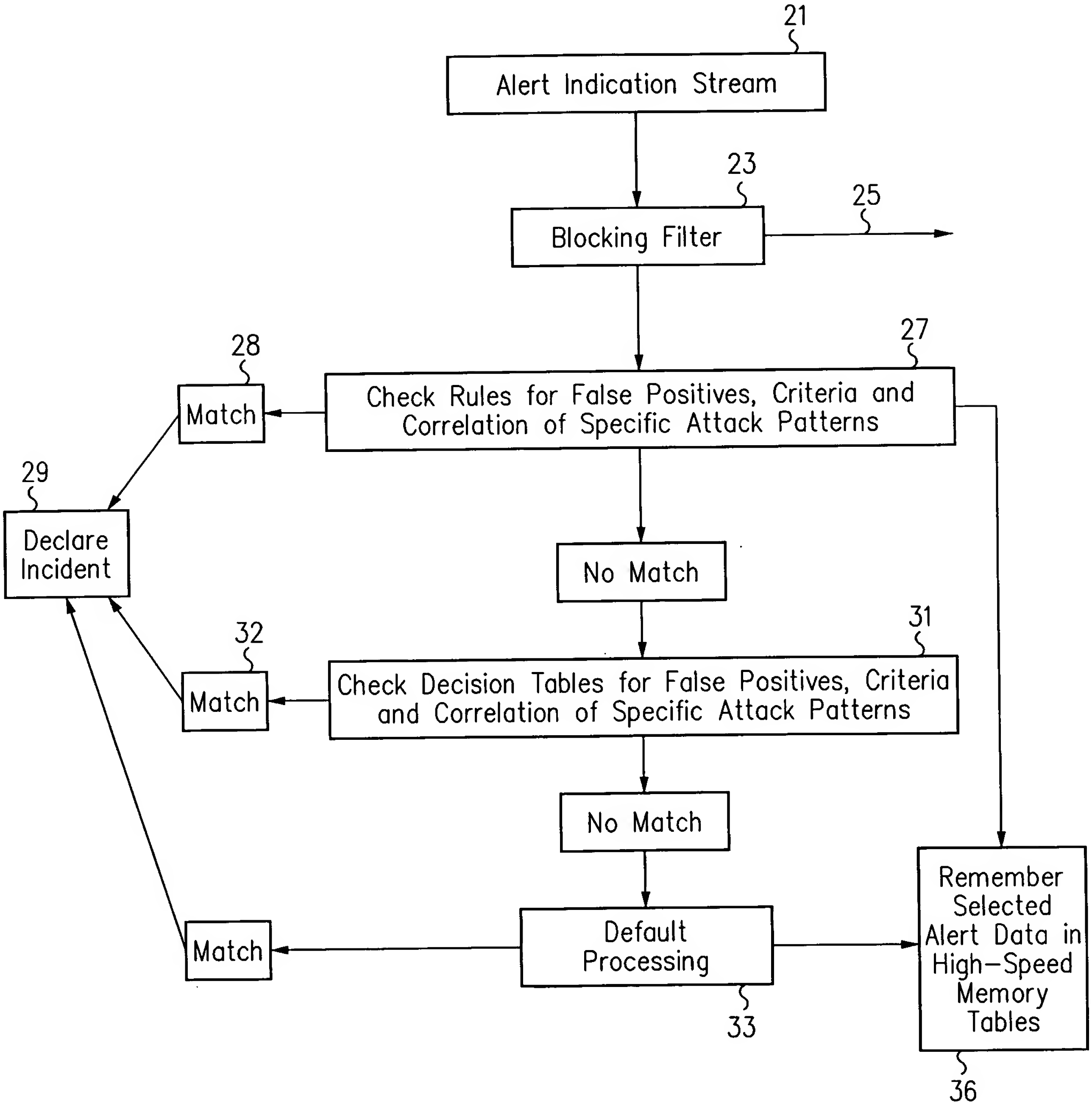
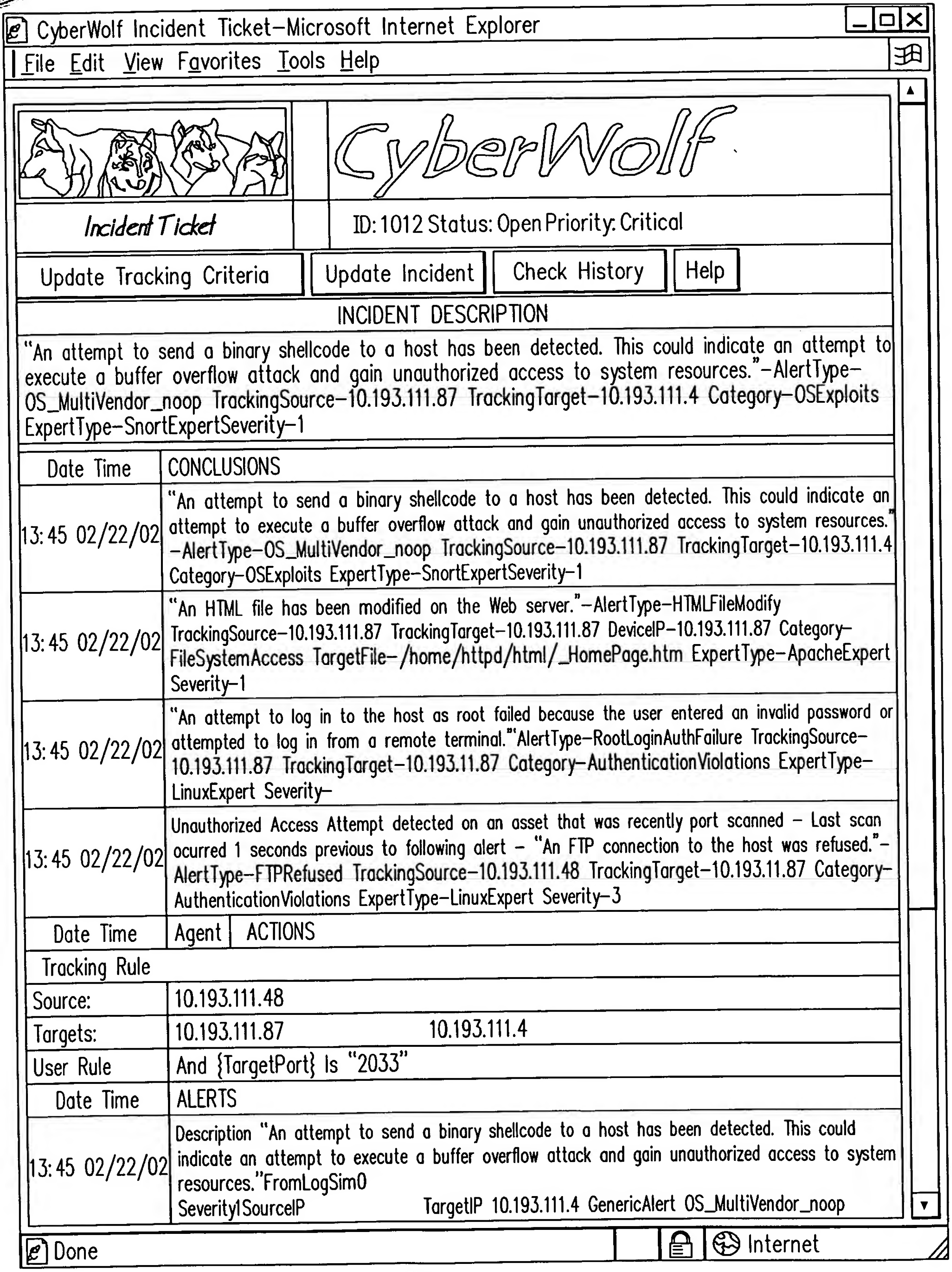

21
Alert Indication Stream
23
Blocking Filter
25
27
Check Rules for False Positives, Criteria and Correlation of Specific Attack Patterns
28
Match
29
Declare Incident
No Match
31
Check Decision Tables for False Positives, Criteria and Correlation of Specific Attack Patterns
32
Match
No Match
Default Processing
33
Match
Remember Selected Alert Data in High-Speed Memory Tables
36

FIG. 3



ID: 1012 Status: Open Priority: Critical

INCIDENT DESCRIPTION

"An attempt to send a binary shellcode to a host has been detected. This could indicate an attempt to execute a buffer overflow attack and gain unauthorized access to system resources."–AlertType–OS_MultiVendor_noop TrackingSource–10.193.111.87 TrackingTarget–10.193.111.4 Category–OSExploits ExpertType–SnortExpertSeverity–1

Date Time	CONCLUSIONS
13:45 02/22/02	"An attempt to send a binary shellcode to a host has been detected. This could indicate an attempt to execute a buffer overflow attack and gain unauthorized access to system resources." –AlertType–OS_MultiVendor_noop TrackingSource–10.193.111.87 TrackingTarget–10.193.111.4 Category–OSExploits ExpertType–SnortExpertSeverity–1
13:45 02/22/02	"An HTML file has been modified on the Web server."–AlertType–HTMLFileModify TrackingSource–10.193.111.87 TrackingTarget–10.193.111.87 DeviceIP–10.193.111.87 Category–FileSystemAccess TargetFile–/home/httpd/html/_HomePage.htm ExpertType–ApacheExpert Severity–1
13:45 02/22/02	"An attempt to log in to the host as root failed because the user entered an invalid password or attempted to log in from a remote terminal."AlertType–RootLoginAuthFailure TrackingSource–10.193.111.87 TrackingTarget–10.193.11.87 Category–AuthenticationViolations ExpertType–LinuxExpert Severity–
13:45 02/22/02	Unauthorized Access Attempt detected on an asset that was recently port scanned – Last scan ocurred 1 seconds previous to following alert – "An FTP connection to the host was refused."–AlertType–FTPRefused TrackingSource–10.193.111.48 TrackingTarget–10.193.11.87 Category–AuthenticationViolations ExpertType–LinuxExpert Severity–3

Date Time	Agent	ACTIONS

Tracking Rule		
Source:	10.193.111.48	
Targets:	10.193.111.87	10.193.111.4
User Rule	And {TargetPort} Is "2033"	

Date Time	ALERTS
13:45 02/22/02	Description "An attempt to send a binary shellcode to a host has been detected. This could indicate an attempt to execute a buffer overflow attack and gain unauthorized access to system resources."FromLogSim0 Severity1SourceIP TargetIP 10.193.111.4 GenericAlert OS_MultiVendor_noop

FIG. 4

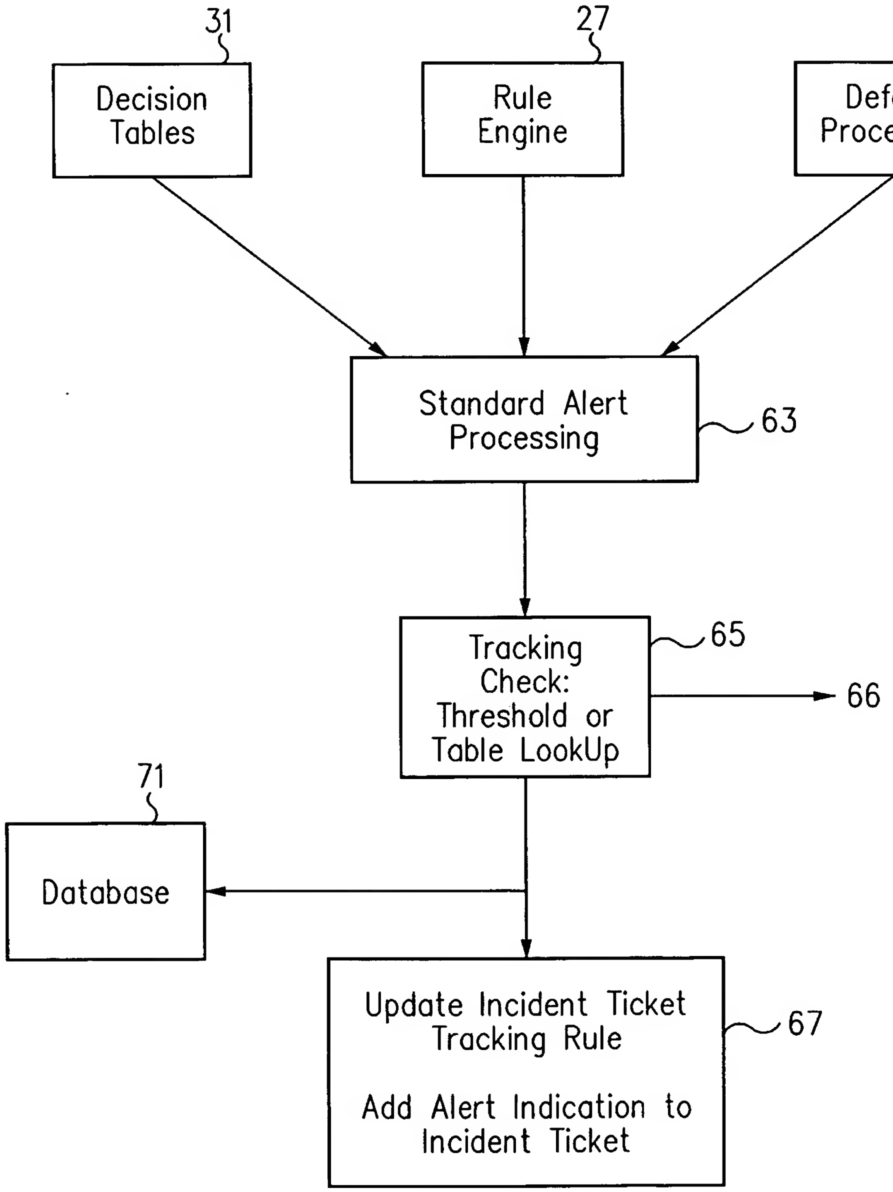
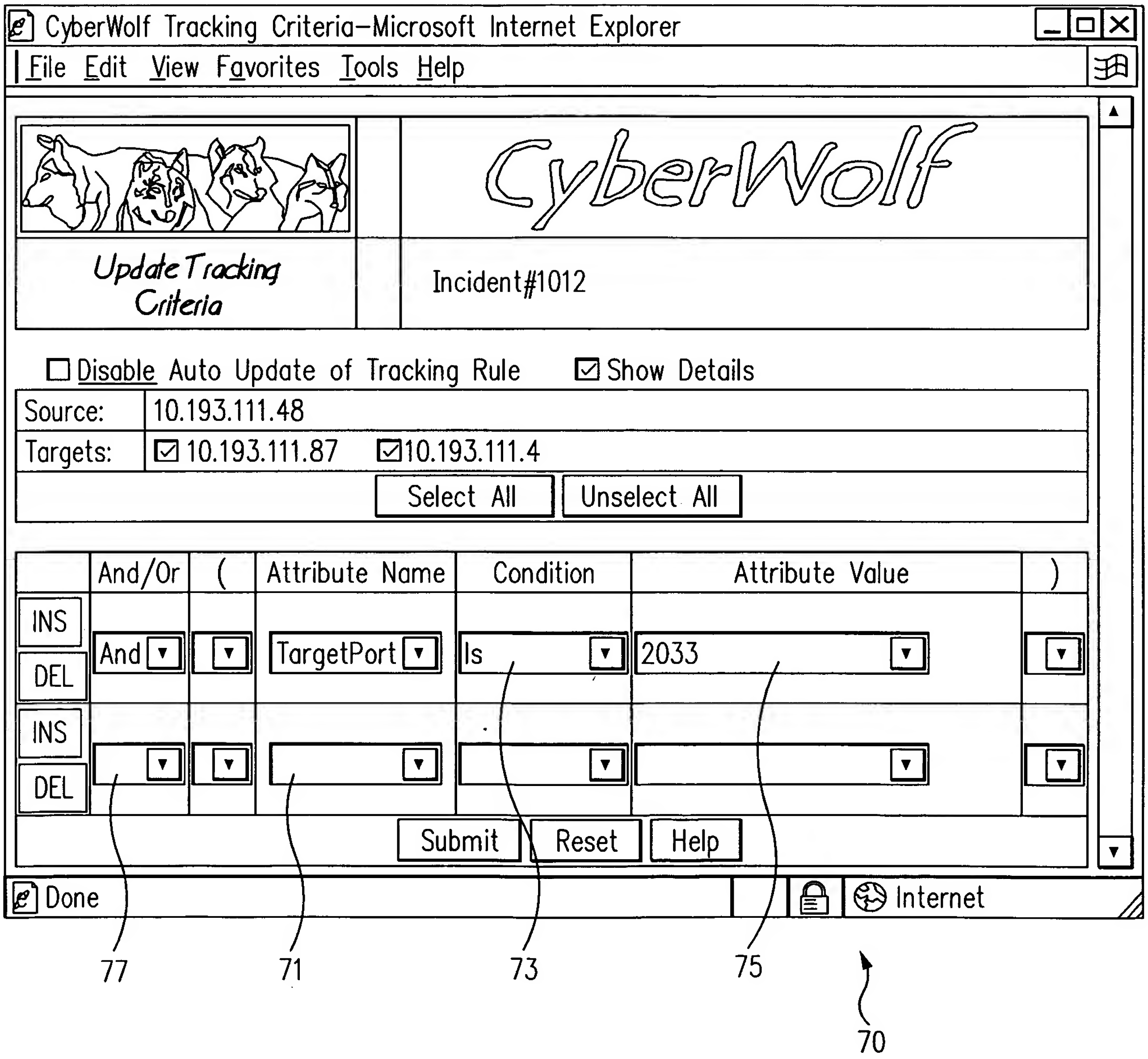

31
Decision Tables
27
Rule Engine
33
Default Processing
Standard Alert Processing
63
Tracking Check: Threshold or Table LookUp
65
66
71
Database
Update Incident Ticket Tracking Rule
Add Alert Indication to Incident Ticket
67

FIG. 5



Incident#1012

☐ Disable Auto Update of Tracking Rule ☑ Show Details

Source:	10.193.111.48
Targets:	☑ 10.193.111.87 ☑ 10.193.111.4

	And/Or	(	Attribute Name	Condition	Attribute Value	)
INS DEL	And		TargetPort	Is	2033	
INS DEL						

FIG. 6